

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of)
HIDAKA et al.)
Application Number: -To be Assigned)
Filed: Concurrently Herewith)
For: METHOD FOR PACKET TRANSFERRING AND)
APPARATUS FOR PACKET TRANSFERRING)

#2
4/26/02
Q2

1c978 U.S. PTO
10/077744
02/20/02

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

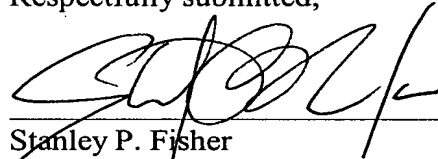
REQUEST FOR PRIORITY
UNDER 35 U.S.C. § 119
AND THE INTERNATIONAL CONVENTION

Sir:

In the matter of the above-captioned application for a United States patent, notice is hereby given that the Applicant claims the priority date of December 4, 2001, the filing date of the corresponding Japanese patent application 2001-369451.

The certified copy of corresponding Japanese patent application 2001-369451 is being submitted herewith. Acknowledgment of receipt of the certified copies is respectfully requested in due course.

Respectfully submitted,



Stanley P. Fisher
Registration Number 24,344

JUAN CARLOS A. MARQUEZ
Registration No. 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200
February 20, 2002

310101409

WN

日 本 国 特 許 庁
JAPAN PATENT OFFICE

Jc978 U.S. PRO
10/077744



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年12月 4日

出 願 番 号

Application Number:

特願2001-369451

[ST.10/C]:

[JP2001-369451]

出 願 人

Applicant(s):

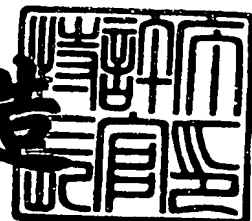
株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3114313

【書類名】 特許願

【整理番号】 H01014091A

【あて先】 特許庁長官 殿

【国際特許分類】 H01L 12/56

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 日高 稔

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 長坂 充

【発明者】

【住所又は居所】 神奈川県横浜市戸塚区戸塚町 2 1 6 番地 株式会社日立製作所通信事業部内

【氏名】 塚田 徳

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【電話番号】 03-3212-1111

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1
【物件名】 要約書 1
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 パケット処理方法および装置

【特許請求の範囲】

【請求項 1】

入力されたパケットフロー毎に該パケットフローを構成するパケットデータに施される処理を選択し、

該パケットデータに選択された処理を施すことを特徴とするパケット処理方法

【請求項 2】

上記パケットフローの入力された入力回線に基づいて、上記処理の選択を行うことを特徴とする請求項 1 記載のパケット処理方法。

【請求項 3】

上記パケットデータに含まれる識別子に基づいて、上記処理の選択を行うことを特徴とする請求項 1 記載のパケット処理方法。

【請求項 4】

上記パケットフローが入力される入力回線と選択すべき処理内容とが対応付けされたテーブルを参照することにより、上記処理の選択を行うことを特徴とする請求項 1 記載のパケット処理方法。

【請求項 5】

上記パケットデータに含まれる識別子と選択すべき処理内容とが対応付けされたテーブルを参照することにより、上記処理の選択を行うことを特徴とする請求項 1 記載のパケット処理方法。

【請求項 6】

パケットデータに施される処理は、カプセル化、デカプセル化、暗号化、復号化、圧縮および伸張のうちから選択される少なくとも一つであることを特徴とする請求項 1 記載のパケット処理方法。

【請求項 7】

入力されたパケットからそのパケットが構成するデータフローの特性を示す識別情報を抽出する処理工程選択部と、

あらかじめ識別情報と上記パケットに施すべき処理の組をデータとして保有する処理選択テーブルと、

上記処理工程選択部で抽出された識別情報をキーとして上記処理選択テーブル情報を検索するテーブル検索部と、

上記テーブル検索結果に従って上記パケットに処理を施すパケット処理部と、
上記処理されたパケットを送出する転送先選択部を有するパケット処理装置。

【請求項 8】

入力されたパケットが持つヘッダ情報からそのパケットが構成するデータフローの特性を示す識別情報を抽出することを特徴とする請求項 7 記載のパケット処理装置。

【請求項 9】

上記データフローの特性を示す識別情報は、送信元アドレスおよび宛先アドレスのうち少なくとも一つであることを特徴とする請求項 8 記載のパケット処理装置。

【請求項 10】

上記パケット処理部は、パケットに施す処理毎に独立した複数種類のパケット処理部であることを特徴とする請求項 8 記載のパケット処理装置。

【請求項 11】

入力されたパケットの発信元を判定する処理工程選択部と、

あらかじめ識別情報と上記パケットに施すべき処理の組をデータとして保有する処理選択テーブルと、

上記処理工程選択部で判定された発信元をキーとして上記処理選択テーブル情報を検索するテーブル検索部と、

上記テーブル検索結果に従って上記パケットに処理を施すパケット処理部と、
上記処理されたパケットを送出する転送先選択部を有するパケット処理装置。

【請求項 12】

パケットが入力された入力回線を上記パケットの発信元として判定することを特徴とする請求項 11 記載のパケット処理装置。

【請求項 13】

入力されたパケットが持つヘッダ情報からそのパケットの発信元を判定することを特徴とする請求項 1 1 記載のパケット処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本願発明は、通信網、特にパケット交換網を構成する通信機器に関する技術分野に関するものである。特に、通信網におけるパケット転送の際にオーバーヘッドなくパケットに処理を施しうる技術に関する。パケットに施される処理としては、情報を秘匿するための暗号化、圧縮、カプセル化などがある。

【0002】

【従来の技術】

図10にパケット転送装置をノードとする通信網の構成例を示す。一般に通信網は、端末（T1,T2,T3,T11など）とノードにより構成される。図10の楕円は複数ノードからなる通信網を表現している。通信の端点として端末同士は通信を行う。通信は端点間をノードで連絡することで、直接接続されていない端末間でも行うことができる。ノードは端末あるいは他のノードとの通信を中継する。通信網の通信を中継する規約がIETF(Internet Engineering Task Force)が定めるインターネットプロトコルに従う通信網をインターネットINと呼ぶ。インターネットINでは、管理者が異なる通信網が相互に接続することにより構成されている。インターネットINのように、管理者が異なるノードからなる網上の通信が広く行われるようになり、管理上、安全性、あるいは運用性の面から端末が属する網の管理者のノードとそれ以外のノードを区別する必要がある。管理者が異なる網間を接続するノードを以下ではエッジノードあるいはエッジルータと呼ぶ。

【0003】

インターネットINを構成する網は、専ら電気通信事業者が管理し不特定多数の利用者の接続を受け入れる網と、利用者が管理しあるいは管理権限を持ち利用者が接続する網がある。後者を以下プライベート網と呼ぶ。前者には専らインターネット接続サービスを利用者に提供する管理者の網と専ら回線接続サービスを利用者に提供する管理者の網とがある。

インターネット接続サービスを利用者に提供する管理者の網を以下ISP網ISP1,ISP2などと呼ぶ。

回線接続サービスを利用者に提供する管理者の網を以下コア網CN1,CN2などと呼ぶ。以下では各網のエッジルータは、プライベート網エッジルータPE1,PE2、ISP網エッジルータER1,ER2、コア網エッジルータCE1,CE2のように呼ぶ。

プライベート網がインターネットに接続する形態は、プライベート網PN1のようにISP網ISP1に直接接続する形態と、プライベート網PN2のようにコア網CN1を介してISP網ISP2に接続する形態とがある。

以上のようなネットワーク上を、データはパケットの形で転送されている。パケット転送方式および装置において、データリンク層の情報、ネットワーク層の情報、トランスポート層の情報など、ネットワークモデル(International Standard Organizationの定めるOSI参照モデル)上で複数層にまたがる情報をパケット転送処理に利用している。

図4にパケットの例を示す。パケットは、トランスポート層データTL_DATAにトランスポート層ヘッダTLHを付加したものがネットワーク層データNL_DATAとなり、ネットワーク層データNL_DATAにネットワーク層ヘッダNLHを付加したものがデータリンク層データDL_DATAとなり、データリンク層データDL_DATAにデータリンク層ヘッダDLHとデータリンク層プロトコルによってはデータリンク層トレーラDLTを付加したものがデータリンク層パケットに成ると云うように入れ子構造に構成される。データリンク層パケットはフレームFLとも呼ばれる。

この入れ子構造をとることをカプセル化と呼ぶ。カプセル化とは一般に、階層化されたネットワークシステムの中で、ある層のプロトコルで扱うパケット、あるいはフレーム全体を、別のプロトコルのヘッダ情報を付加することで、ペイロードとして扱う手法をいう。逆にヘッダを削除し包まれたデータを取り出すことをデカプセル化と呼ぶ。

【0004】

パケット転送を行う際の処理には、ノードが該当する層のヘッダ処理を行うだけでこと足る場合とパケットデータ全体を処理する必要がある場合とがある。ヘッダ処理の例は、ネットワーク層の経路選択である。この場合、ネットワーク

層ヘッダを処理することで出力先を決定できる。一方、パケット全体の処理を必要とする場合があり、その例は、パケットの暗号化、復号化、カプセル化あるいはデカプセル化などである。

【 0 0 0 5 】

また、プライベート網は、トンネリング技術を用いて仮想的に接続することもできる。ここでトンネリングの為のカプセル化を説明する。トンネリングとは、図 1 を例として説明すると、端末 T1 と端末 T3 が通信するパケットをエッジルータ PE1 とエッジルータ PE3 が通信するパケットにカプセル化することで、端末が通信するパケットは図 1 の破線で示した経路のエッジルータ PE1 と PE3 間の経路を仮想的に接続された経路と見なす方式である。この仮想的に接続された経路はトンネル TN1 と呼ばれる。トンネリングの具体的な方式は、新たなヘッダによりパケットをカプセル化することにより被カプセル化パケットの処理層の処理を新たなヘッダによる転送処理で行うことである。図 1 の例の場合、トンネリングとは、エッジルータ PE1 が、端末 T1 が送信したパケットに新たなネットワーク層ヘッダを付加し、その付加したネットワーク層ヘッダの情報による転送で到着するエッジルータ PE3 が、エッジルータ PE1 が付加したヘッダを削除し端末 T1 が送信したパケットを取り出すことである。

【 0 0 0 6 】

図 5 にネットワーク層のパケットをネットワーク層でカプセル化するパケット構成例を示す。カプセル化では、図 4 で示したネットワーク層ヘッダ NLH を持つデータリンク層データ DL_DATA であるパケットを新たなネットワーク層データ T_NL_DATA とし、新たなネットワーク層ヘッダ T_NLH を付加し、その部分が新たなデータリンク層データ DL_DATA2 と成る。このデータリンク層データ DL_DATA2 はデカプセル化されるまで、このネットワーク層ヘッダ T_NLH の情報を基にしたネットワーク層のパケットとして処理される。デカプセル化では、このネットワーク層ヘッダ T_NLH の情報を基にして到着した宛先ノードでネットワーク層ヘッダ T_NLH が削除され、そのネットワーク層データ T_NL_DATA がもとのネットワーク層のパケット、つまりもとのデータリンク層データ DL_DATA として復元される。復元されたデータは、ネットワーク層ヘッダ NLH の情報でネットワーク層のパケットし

て転送される。

【0007】

端末が通信する場合、トランスポート層より下位層で送受信するデータは個々のパケットであるが、セッション層より上位層で送受信するデータは連続したパケットから成るパケット群である。このパケット群を以下パケットフローと呼ぶ。

【0008】

【発明が解決しようとする課題】

図1のネットワークを上記パケットフローが転送される際に、データの内容秘匿のための暗号化技術が重要となる。

【0009】

従来、IETFが発行するRequest For Comments(RFC)2406 IP Encapsulating Security Payloadで行われているように、暗号化処理は、パケットフロー毎に端末上の応用プログラムが個別に処理したり、またはノードが暗号化を行っていた。暗号化にはパケットのデータ部を暗号化する場合と、トンネリング（カプセル化）を行い、プライベート網内の転送情報であるネットワーク層ヘッダも含めたパケットデータ全体を暗号化する場合がある。パケットデータ全体を暗号化するのは、インターネットではパケットは管理者が特定できない経路を通過するため経路の安全性や経路情報の秘匿性を守る観点から、端末が属するプライベート網内のネットワーク層ヘッダ内の転送情報を、パケットが通過する経路のノード上でパケットを認識可能な者から秘匿する必要があるためである。

【0010】

図5と図6を用いて、暗号化のためにパケットをカプセル化する例を説明する。図6に暗号化したトンネリングの為にネットワーク層ヘッダも含めて暗号化されたパケットの構成例を示す。カプセル化されたパケットT_NL_DATAがISP網をトンネルして通過するために必要な処理として、新たなネットワーク層ヘッダT_NLHがカプセル化ヘッダとしてパケットに付加される。暗号化の場合、カプセル化されるデータT_NL_DATAは、暗号化されたカプセル化データENCRYPTEDとして暗号化される。このようにプライベート網内のアドレス情報を持つネットワーク層ヘッ

ダNLHは暗号化され、ISP網内で通過するノードでは暗号化されたデータENCRYPTEDとして転送されるので、第三者がネットワーク層ヘッダNLHの値を得ることは困難である。

【 0 0 1 1 】

パケットは、パケットフローとしてノードを通過する。従来のパケット転送装置で暗号化あるいは復号化を行う場合、対向パケット転送装置までの経路上を通過するパケットフロー毎に処理を行っている。またこの場合、エッジノードは、トンネル経路すなわちパケットを復号化する相手エッジノードまでの経路を通過するパケットを一様に暗号化していた。

このような従来のパケット転送装置においては、パケットフローを生成した端末を識別してパケットフロー中の暗号化あるいは復号化の要否を判断し、暗号化が必要なパケットのみに暗号化処理することは行っていない。

パケット転送装置をエッジノードとした場合、そのエッジノードが属する網のパケットフローが集中して通過する。エッジノードがパケットヘッダ処理に比較して計算量の多い暗号化処理を実行する場合、パケットフローが集中するノードでは計算による遅延でパケットの処理量が制限される。そこでパケットの処理量を効率化する必要がある。

【 0 0 1 2 】

【課題を解決するための手段】

そこで本発明のパケット転送装置では、パケットフロー毎に利用者あるいは処理内容を識別する識別手段を具備する。またパケットフロー状態を識別してパケットフローを構成するパケットデータへの処理を変更あるいは選択する手段を具備する。また暗号化などパケットに施す処理の要否を判断する手段を具備する。またパケット転送処理において、パケット情報、装置の内部状態に従って処理を変更することが可能な手段を具備する。

【 0 0 1 3 】

識別手段は、入力パケットが持つヘッダ情報から宛先情報等を抽出し、その入力パケットが構成するパケットフローの状態を把握する処理判別部と判別部の結果を保持したテーブル情報検索部とパケットに施す処理を決定する部分とパケッ

トに施す処理ごとに専用処理部を有する。

【0014】

より具体的には、本発明のパケット処理方法では、入力されたパケットフロー毎にパケットフローを構成するパケットデータに施される処理を選択し、パケットデータに選択された処理を施す。処理の選択は、パケットフローの入力された入力回線に基づいて、あるいは、パケットデータに含まれる識別子に基づいて、行うことができる。具体的には、パケットフローが入力される入力回線やパケットデータに含まれる識別子と、選択すべき処理内容とが対応付けされたテーブルを参照することにより、処理の選択を行う。パケットデータに施される処理は、例えばカプセル化、デカプセル化、暗号化、復号化、圧縮および伸張等種々の処理のうちから選択される一つ、あるいは、これらの組み合わせである。

本発明によるネットワークシステムは、複数の通信網と、各通信網に属する端末と、通信も間を中継するエッジノードを有し、端末間をパケットフローがエッジノードを介して通信され、エッジノードはパケットフローの特性（例えば利用者、送信元、受信先、要求される処理など）に応じて、選択的にパケットフローに処理を施す。処理の典型例は、暗号化である。暗号化にはデータ部分のみの暗号化とカプセル化を含む。

さらに本発明になるエッジノードの構成としては、入力されたパケットからそのパケットが構成するデータフローの特性を示す識別情報を抽出する処理工程選択部と、あらかじめ識別情報とパケットに施すべき処理の組をデータとして保有する処理選択テーブルと、処理工程選択部で抽出された識別情報をキーとして処理選択テーブル情報を検索するテーブル検索部と、テーブル検索結果に従ってパケットに処理を施す独立したパケット処理部と、処理されたパケットを送出する転送先選択部を有するパケット処理装置を備える。入力されたパケットが持つヘッダ情報からそのパケットが構成するデータフローの特性を示す識別情報を抽出ができる。これは例えば、送信元アドレスや宛先アドレス等の利用者情報である。

【0015】

別の例としては、入力されたパケットの発信元を判定する処理工程選択部と、あらかじめ識別情報とパケットに施すべき処理の組をデータとして保有する処理

選択テーブルと、処理工程選択部で判定された発信元をキーとして処理選択テーブル情報を検索するテーブル検索部と、テーブル検索結果に従ってパケットに処理を施す独立したパケット処理部と、処理されたパケットを送出する転送先選択部を有するパケット処理装置である。ここで、パケットが入力された入力回線をパケットの発信元として判定したり、入力されたパケットが持つヘッダ情報からそのパケットの発信元を判定したりすることができる。

【 0 0 1 6 】

【発明の実施の形態】

図 2 により本発明を適用したパケット転送装置すなわちエッジノードの構成例を説明する。エッジノードとは例えば、図 1 のプライベート網エッジルータ PE1、PE2、ISP 網エッジルータ ER1、ER2、コア網エッジルータ CE1、CE2 などである。エッジノードは、装置外部から図 5、図 6 に示すデータリンク層のパケットを受信する入力回線を収容した入力回線インタフェース 30-1、30-n と装置外部へデータリンク層のパケットを送信する出力回線を収容した出力回線インタフェース 50-1、50-n と、入力回線インタフェースが受信したデータリンク層のパケットを処理する入力処理部 13-1、13-m と、入力処理部から出力処理部へ装置内でデータを転送するスイッチ部 12 と、送信するデータリンク層のパケットを処理する出力処理部 14-1、14-m と、これらを制御する制御部 11 から成る。入力回線、出力回線、入力回線インタフェース、出力回線インタフェース、入力処理部、出力処理部、スイッチ部、制御部はパケット転送装置にそれぞれ複数備えることも可能である。

【 0 0 1 7 】

入力回線インタフェース 30-1、30-n は、入力回線から入力された物理信号をデータリンク層パケット認識し、データリンク層パケットを入力パケット処理部 20 へ転送する。

【 0 0 1 8 】

入力パケット処理部 20 は入力されたデータリンク層パケットを処理し、処理したパケットをスイッチ部 12 に転送する。スイッチ部 12 は入力パケット処理部 20 から転送されたパケットを出力パケット処理部 40 へ転送する。出力パケット処理部 40 はスイッチ部 12 から転送されたパケットを処理し、データリンク層パケットと

して出力回線インターフェース50-1,50-nへ転送する。

【0019】

出力回線インターフェース50は、出力パケット処理部40から転送されたデータリンク層パケットを受信し出力回線へ適した物理信号に変換して出力する。

【0020】

図3により入力パケット処理部20と出力パケット処理部40の構成例を説明する。入力パケット処理部20は、少なくとも一つの演算装置CPUと記憶装置MSと複数の入出力装置205からなる。入出力装置205は、演算装置CPU1、演算装置CPU2等、あるいは記憶装置MSと、入出力回線インターフェース、スイッチ部あるいは制御部とを、バスあるいはクロスバススイッチにより接続する。本実施例の入力パケット処理部20と出力パケット処理部40は類似の構成であり、連携してパケットを処理する。

【0021】

図9に本発明を適用したパケット転送装置の論理構成図を示す。これらの構成は、図3の一つあるいは複数のCPU1、CPU2上のデータ処理及び記憶装置MSによって実現することができる。しかし、すべてハードウェア構成とすることもできる。本方式は、入力インターフェース部あるいはスイッチ部から入力されたパケットが持つヘッダ情報を抽出し、そのパケットが構成するデータフローの状態を把握する処理工程選択部100とテーブル情報の更新の管理を行うテーブル管理部101とテーブル情報を検索するテーブル検索部102と通信網内の認証サービスとの間で行う認証処理結果をテーブル管理部へ伝える認証処理部103とテーブル104とテーブル検索結果によりパケットに施す処理毎のパケット処理部300とスイッチ部あるいは出力インターフェース部へパケットを転送する転送先選択部400を有する。

【0022】

処理工程選択部100では、入力パケットのデータリンク層ヘッダDLH、あるいはトレイラDLTに含まれる情報からデータリンク層識別子IN12を得る。また、ネットワーク層ヘッダNLHに含まれる情報からネットワーク層識別子IN21を得る。また、トランスポート層ヘッダTLHに含まれる情報からトランスポート層識別子IN22を得る(図4、図5、図7、図8参照)。例えばデータリンク層識別子は、データ

リンク層の送信元アドレス、宛先アドレス、およびセッション識別子である。例えば、RFC2516で示されるPPP over Ethernetでは、入力パケットのデータリンク層ヘッダDLHからセッション識別子が得られる。またネットワーク層識別子はネットワーク層の送信元アドレス、宛先アドレス、上位層プロトコル識別子である。ネットワーク層ヘッダの例は、RFC791で示されるInternet Protocol(IP)である。またトランスポート層で抽出する情報はトランスポート層アドレスやトランスポート層状態フラグである。トランスポート層ヘッダの例は、RFC793で示されるTCPやRFC768で示されるUDPである。入力パケットを発信した端末は、入力回線IN11、データリンク層識別子IN12あるいはネットワーク層識別子IN21により特定する。

【 0 0 2 3 】

テーブル検索部102では、入力処理工程選択部100が入力パケットから抽出した入力情報IN1あるいは入力情報IN2を検索キーにして出力情報を記録したテーブルを検索する。

処理工程選択部100は、テーブル検索部102から得た検索結果すなわち出力情報OUT1と出力情報OUT2に応じ、パケット処理部300へデータ処理を指示する。

【 0 0 2 4 】

図7にデータリンク層ヘッダの情報をパケットフロー識別に利用するテーブルの例を、図8にネットワーク層ヘッダの情報とトランスポート層ヘッダの情報の一方または両方をパケットフロー識別に利用するテーブルの例を示す。

図7の例では、入力パケットから得られた入力回線IN11や入力データリンク層識別子IN12から入力情報IN1が構成される。入力情報IN1を検索キーとし図7に示したテーブルの検索を行うことで出力情報OUT1を得る。出力情報OUT1は、パケットが出力される出力回線OUT11、出力データリンク層識別子OUT12、データリンク層(DL)状態OUT13、パケット通過条件OUT14から構成する。また、処理識別子OUT15によりパケットに行う処理が指定される。

図8の例では、入力パケットから得られた入力ネットワーク(NL)層識別子IN21や入力トランスポート(TL)層識別子IN22から入力情報IN2が構成される。入力情報IN2を検索キーとし図8に示したテーブルの検索を行うことで出力情報OUT2を

得る。出力情報OUT2は、出力ネットワーク層（NL）識別子OUT11、トランスポート層（TL）状態OUT22、パケット通過条件OUT23、処理識別子OUT24、および出力データリンク層識別子OUT25から構成する。

図1のプライベート網エッジルータPE1は、入力パケットの発信端末を、入力データリンク層識別子IN12で識別できる。図7の例では、端末T1の通信するパケットであることは、入力処理工程選択部がパケット抽出した入力情報IN1を検索キーとして図7に示したテーブルを検索することで判断できる。すなわち端末T1の発信したパケットは、入力データリンク層識別子IN12が0002であり、端末T11の発信したパケットは入力データリンク層識別子IN12が0010であるので発信端末が識別できる。

また、図7の例では、端末T1のパケットフローは、認証処理部103が利用者識別した入力回線IN11、入力データリンク層識別子（セッション識別子）IN12毎に、テーブルエントリのDL状態OUT13をデータ通信に変更することで判断できる。出力回線がどの網に接続しているかはテーブルエントリに保持された出力データリンク層識別子（セッション識別子）OUT12から識別する。同様に端末T11の通信するパケットであることも識別できる。そこで端末に応じた処理識別子OUT15を割り当てることにより暗号化の要否の判断を行うことが出来る。

【 0 0 2 5 】

テーブル管理部102は、処理工程選択部100が抽出した情報からデータリンク層状態の変更、パケット通過条件変更を判定し、テーブルエントリに設定する。また、暗号化等の処理の要否を判定し、処理識別子をテーブルエントリに設定する。図7の例では、テーブルエントリのデータリンク層（DL）状態OUT11は、入力データリンク層識別子IN12毎のデータリンク層パケットの到着履歴である。また、図8の例では、トランスポート層（TL）状態OUT21は、入力トランスポート層識別子IN22毎のトランスポート層パケットの到着履歴である。

【 0 0 2 6 】

認証処理部103は、パケット転送装置外部の認証サービス、あるいは図示していないパケット転送装置内部の認証サービスと通信し利用者の認証を行う。入力パケットはそのパケットを生成した利用者情報を含む。利用者情報は、データリ

ンク層識別子やネットワーク層識別子やトランスポート層データに含まれる上位層の情報である。そこで認証処理部は、その利用者情報を認証サービスに送信し、認証結果を受信する。認証処理部は認証結果に従いそのパケットが属するパケットフローのテーブルエントリを登録、抹消、パケット通過条件OUT14の変更の要否をテーブル管理部に通知する。テーブル部はエントリとしてその情報を保持する。

【 0 0 2 7 】

パケット処理部300は、処理識別子により選択されて実行される。

本発明のパケット転送装置をエッジルータとして用いた網の構成例である図1を用いて、パケット処理部300を説明する。第一のプライベート網PN1のエッジルータPE1と第三のプライベート網PN3のエッジルータPE3はコア網CN1を介して第一のISP網ISP1のエッジルータER1と接続し、第二のプライベート網PN2のエッジルータPE2はコア網CN2を介して第二のISP網ISP2のエッジルータER5と接続する。また、プライベート網PN1とプライベート網PN2はトンネルTN2で接続されている。プライベート網1とプライベート網PN3はトンネルTN1で接続されている。

【 0 0 2 8 】

図1を再度参照して、広域ネットワークに於ける本願発明の動作を説明する。

図1のプライベート網エッジルータPE1が送信するパケットは、図8のテーブルを用いると、通信相手が図の破線すなわち契約ISP内の暗号化が不要な経路(トンネルTN1)で接続される端末T3である場合、処理識別子OUT15によりトンネリングの為のカプセル化処理301が選択される。通信相手が図の一点鎖線すなわちインターネットINを通過し暗号化が必要な経路(トンネルTN2)で接続される端末T2である場合、処理識別子により暗号化処理部303が選択され、さらにトンネリングの為のカプセル化処理301が選択される。

一方プライベート網エッジルータPE1が受信するパケットは、図8のテーブルを用いると、通信相手が図の破線すなわち契約ISP内の暗号化が不要な経路(トンネルTN1)で接続される端末T3である場合、処理識別子OUT15によりトンネリングの為のデカプセル化処理302が選択される。通信相手が図の一点鎖線すなわちインターネットINを通過し暗号化が必要な経路(トンネルTN2)で接続される端末T2

である場合、処理識別子によりトンネリングの為のデカプセル化処理302が選択され、さらに複号化処理部304が選択される。また、パケットにデータ圧縮伸張処理が必要な場合には、圧縮処理部305あるいは伸張処理部306へパケットが転送される。必要な処理が終了するとパケット処理部300は転送先選択部400にパケットデータを送信する。転送先選択部400では、パケットデータをスイッチ部12または出力回線インタフェース50へ転送する。また、処理工程選択部100では、スイッチ部12から転送されたパケットの場合も同様な処理を行う。

【0029】

図11により、本発明のパケット転送装置を用い、ISP網側のエッジルータにより、仮想プライベート網VPNを構成する場合の実施例を説明する。この場合、プライベート網内のパケットは、ISP網のエッジルータER2によりカプセル化されトンネル用のパケットとなる。ISP網のエッジルータER2は、ISP網を通過するために必要な新たなネットワーク層ヘッダT_NLHをカプセル化ヘッダとしてパケットに付加する。接続契約しているプライベート網PN1のエッジルータPE1からのパケットはデータリンク層識別子とネットワーク層識別子により端末T1からのパケットであることを認識できる。同様に端末T11からのパケットであることも認識できる。暗号化は、テーブルに保持した処理識別子に従って行う。この場合、インターネット接続サービスを行う事業者は、その事業者の管理するISP網ISP1に接続する利用者に代わって暗号化したトンネリング等の付加価値サービスを行うことが出来る。

【0030】

【発明の効果】

本発明により、入力パケットの発信端末あるいは利用者を認識することが可能であり、送信先の判定も可能であるので、利用者あるいは処理内容を識別してパケットの処理を変更し、パケットフローを構成するパケット処理を変更しエッジノードを通過するパケットの処理を差別化することが可能である。また、利用者が暗号化を行いたいパケットを選択的に暗号化することができ、利用者毎に暗号化が必要な経路を通過するパケットのみを暗号化することができる。従って、エッジノードで暗号化等の比較的計算量の多い処理を選択的に行うことが可能とな

る。高速回線を収容したパケット転送装置によりデータフローの暗号化処理を行うことが可能となることで、パケットがプライベート網の管理者以外の管理する網を通過する場合にもプライベート網内の宛先情報が秘匿されるので、プライベート網内の宛先にサービス不能攻撃などの悪意あるアクセスが行い難くなる。本方式を具備したパケット転送装置の管理者は、利用者毎にパケット処理を差別化したサービスを提供することが可能である。

【図面の簡単な説明】

【図 1】

本発明によるエッジノードを用いた網の構成例を説明する概念図である。

【図 2】

本発明によるエッジノードの構成例を説明するブロック図である。

【図 3】

本発明によるエッジノードのパケット処理部の構成例を説明するブロック図である。

【図 4】

パケットの構成例を説明する概念図である。

【図 5】

カプセル化されたパケットの構成例を説明する概念図である。

【図 6】

カプセル化されデータ部を暗号化したパケットの構成例を説明する概念図である。

【図 7】

本発明による処理工程選択に用いるテーブル構成を説明する表図である。

【図 8】

本発明による処理工程選択に用いるテーブル構成を説明する表図である。

【図 9】

本発明によるエッジノードのパケット処理部の論理構成例を説明するブロック図である。

【図10】

本発明によるエッジノードを用いた網の構成例を説明する概念図である。

【図11】

本発明によるエッジノードを用いた網の構成例を説明する概念図である。

【符号の説明】

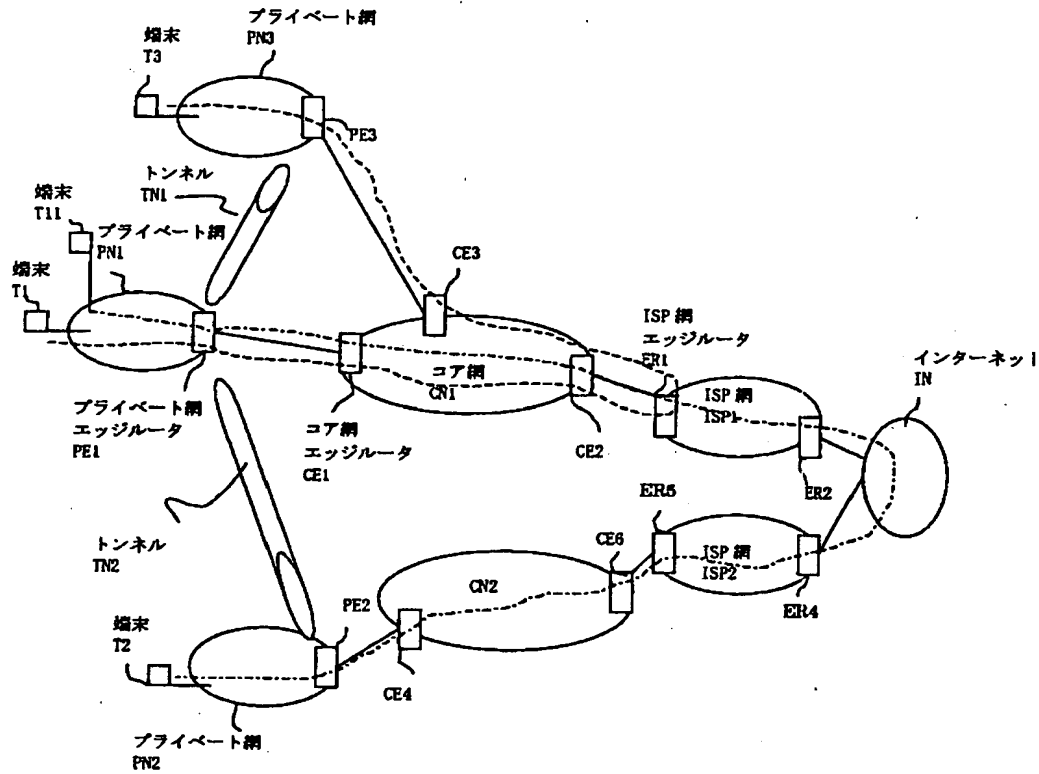
T1…端末、DT1…ダイヤルアップ端末、PN1…プライベート網、ISP1…ISP網、CN1…コア網、PE1…プライベート網エッジルータ、ER1…ISP網エッジルータ、CE1…コア網エッジルータ、IN…インターネット、TN1…トンネル、11…制御部、12…スイッチ部、13…入力処理部、14…出力処理部、20…入力パケット処理部、30…入力回線インタフェース、40…出力パケット処理部、50…出力回線インタフェース、100…入力処理工程選択部、101

DLH…データリンク層ヘッダ、DLT…データリンク層トレーラ、DL_DATA…データリンク層データ、NLH…ネットワーク層ヘッダ、NL_DATA…ネットワーク層データ、T_NLH…ネットワーク層ヘッダ、T_NL_DATA…ネットワーク層データ、TLH…トランスポート層ヘッダ、TL_DATA…トランスポート層データ、FL…データリンク層パケットまたはフレーム。

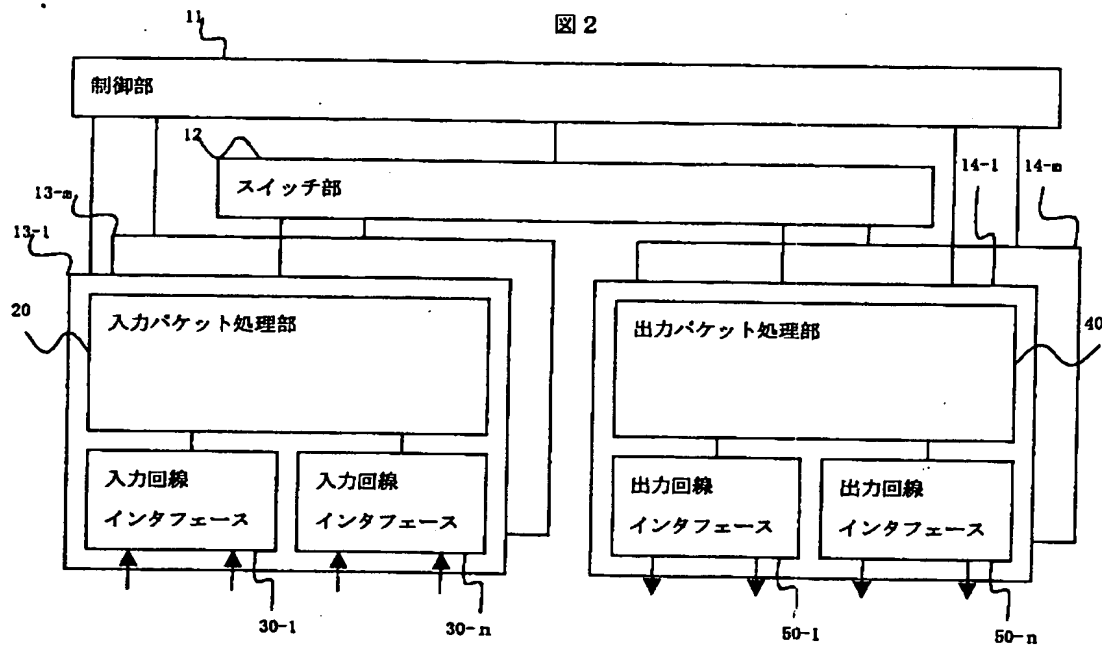
【書類名】 図面

【図 1】

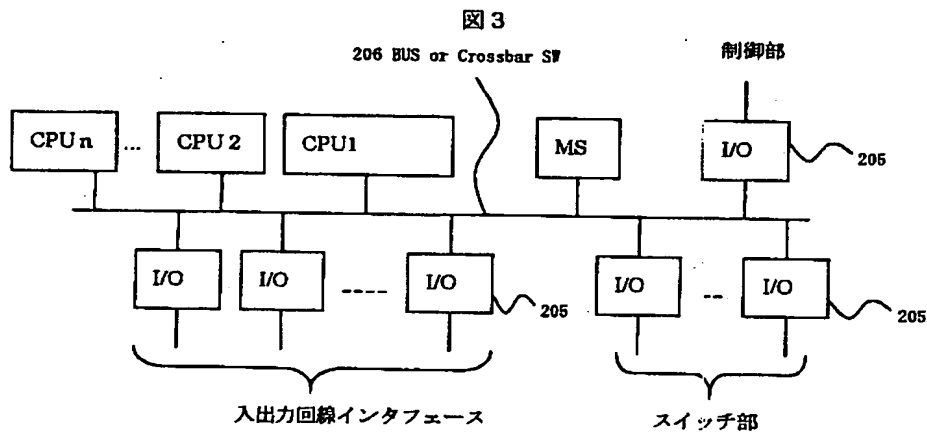
図 1



【図 2】

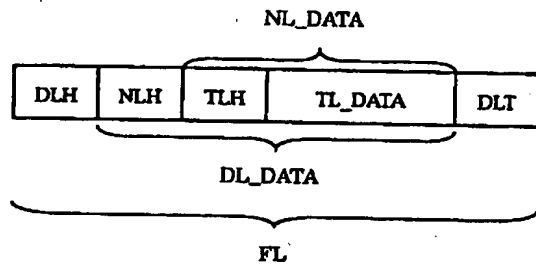


【図 3】



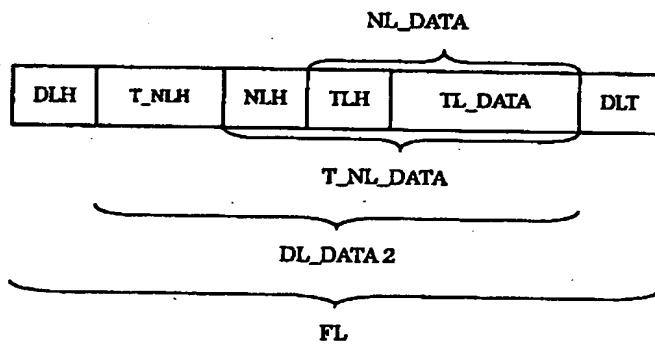
【図 4】

図 4



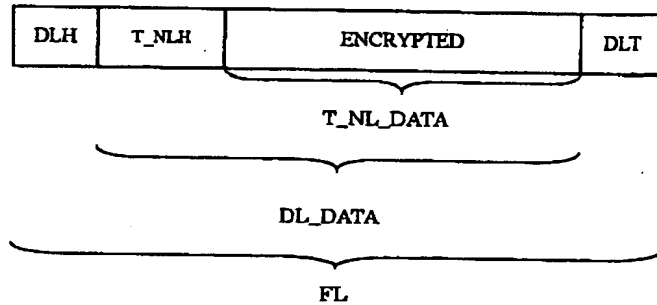
【図 5】

図 5



【図 6】

図 6



【図 7】

図 7

入力情報		出力情報				
入力回 線	入力 DL 識別 子	出力回 線	出力 DL 識別 子	DL 状態	パケット通過条件	処理識別子
1	0002	2	0004	データ通信	0021	1001
1	0011	-	-	リンク確立	8021,C021,C023	0002
1	0010	2	0004	データ通信	0021	1002
2	0005	-	-	リンク確立	8021,C021,C023	0003
2	0004	1	0002	データ通信	0021	1003

IN11 IN12 OUT11 OUT12 OUT13 OUT14 OUT15

【図 8】

図 8

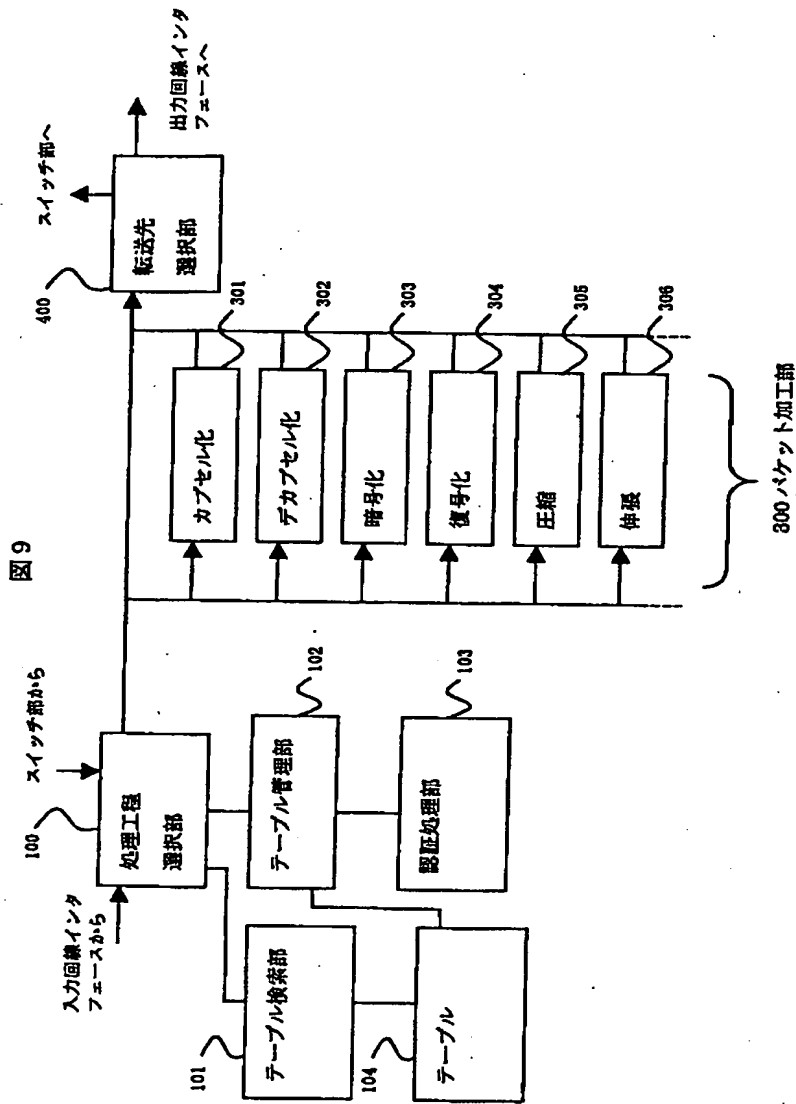
入力情報		出力情報				
入力 NL 識別子	入力 TL 識別子	出力 NL 識別子	TL 状態	パケット通過条件	処理識別子	出力 DL 識別子
0001	-	0002	-	-	-	0004
0001	-	0003	-	-	0003	0004
0002	-	0001	-	-	-	0002
0003	-	0001	-	-	-	0002
0011	0004	0002	TCP SYN 待ち	TCP DP 1020	-	0004
0011	0004	0002	TCP ACK 待ち	TCP DP 1020	0005	0004
0005	0004	0004	TCP SYN 待ち	TCP SP 1020	-	0004
0005	0004	0004	TCP ACK 待ち	TCP SP 1020	0005	0004

IN2

OUT2

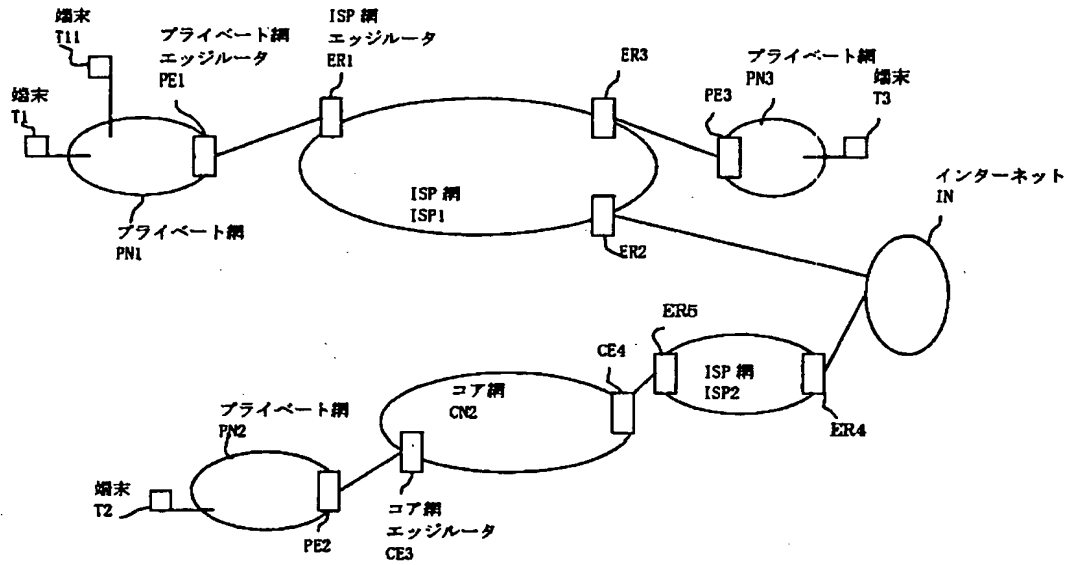
IN21 IN22 OUT21 OUT22 OUT23 OUT24 OUT25

【図9】



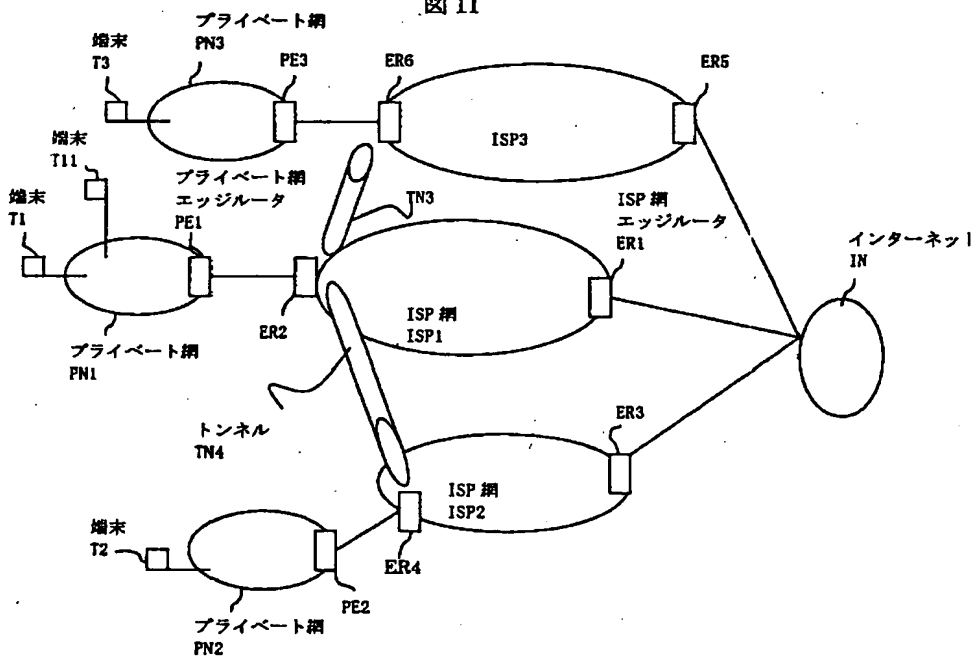
【図10】

図10



【図11】

図11



【書類名】 要約書

【要約】

【課題】 通信網中のデータフローの集中するエッジノードで暗号化等の計算量が多く負荷が高いサービスを行う場合に高速回線を収容可能なパケット転送方式あるいは装置を実現する。

【解決手段】 入力パケットから得られた情報を装置内テーブルエントリに保持し、入力パケットの発信元あるいは出力先あるいは装置内部の状態に応じて暗号化等の処理の要否を判断することで暗号化等の必要なパケットだけに処理を施すことで計算量を削減する。

【選択図】 図1

特2001-369451

認定・付加情報

特許出願の番号	特願2001-369451
受付番号	50101776557
書類名	特許願
担当官	第五担当上席 0094
作成日	平成13年12月 5日

<認定情報・付加情報>

【提出日】	平成13年12月 4日
-------	-------------

次頁無

出 願 人 履 歴 情 報

識別番号

[000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所